

A Survey on SCADA / Distributed Control System Current Security Development and Studies

Alper Ozbilen, Prof. Dr. İlhami Colak and Prof. Dr. Seref Sagirolu

Gazi University, Technology Faculty
Electrical Education Department
Teknikokullar, Ankara
TURKEY

aobilen@btk.gov.tr / icolak@gazi.edu.tr / ss@gazi.edu.tr

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems and other distributed control systems, are widely used in critical infrastructure and industrial plants. In recent times, many distinguished newspapers, magazines and reports publicized successful intrusions and attacks on SCADA based systems to bring security issues of critical infrastructure to the agenda. Recent various studies and assessments on control systems incidents indicate that these systems will increasingly become a greater target for cyber attacks, denial of service and physical disruption.

This paper will discuss a variety of SCADA security issue publicized in worthy recent reports. It will also recommend some emerge measures and further studies fields in order to provide more secure control system network design.

1.0 INTRODUCTION

Protection of critical infrastructure such as water, power, energy, and telecommunication is vital because of impact such destruction would have on casualties, the economy, the psychology, and the pride of nation [1]. When SCADA systems are used in critical infrastructure installations, it is important to consider security requirements. Some legislation studies and In section 2 and 3

SCADA based systems usually maintain significant control over core infrastructure and the disruption of these services could have catastrophic events. So SCADA systems securities have been became more of an issue in recent years. In energy sector considered as most critical part of national infrastructure, they are crucial part of whole system as controlling equipment ranging from valves in oil and gas pipelines to switches and breakers in the national electric grid. Because of the importance, attackers, most of whom are politically motivated, could utilize these control systems to cause catastrophic damage or outages.

Some country and international organization have already started to spent great effort to asses security needs and criticality of infrastructures. In Section 2, some legislative studies in the USA and EU are reviewed to show concerns about vulnerabilities of critical infrastructures.

Most SCADA system designs did not anticipate the security threats posed by today reliance on common software and operating systems, public telecommunication networks, and internet [2]. Although SCADA systems have historically been isolated from other computer system like enterprise computer network or internet, it have been interconnecting with enterprise network by spread with TCP/IP as a carrier protocol [3]. In addition, general purpose operating system (OS) like Windows and Linux have started to be used mostly in new SCADA system. This have been led to emerge new vulnerabilities while property OS have been incapable of performing emerging security mechanism. Various studies and assessments have revealed that there is a lack of security in SCADA systems.

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE NOV 2010		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE A Survey on SCADA / Distributed Control System Current Security Development and Studies				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Gazi University, Technology Faculty Electrical Education Department Teknikokullar, Ankara TURKEY				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091					
14. ABSTRACT Supervisory Control and Data Acquisition (SCADA) systems and other distributed control systems, are widely used in critical infrastructure and industrial plants. In recent times, many distinguished newspapers, magazines and reports publicized successful intrusions and attacks on SCADA based systems to bring security issues of critical infrastructure to the agenda. Recent various studies and assessments on control systems incidents indicate that these systems will increasingly become a greater target for cyber attacks, denial of service and physical disruption. This paper will discuss a variety of SCADA security issue publicized in worthy recent reports. It will also recommend some emerge measures and further studies fields in order to provide more secure control system network design.					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT SAR	18. NUMBER OF PAGES 12	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

The most of systems owners and operators are be reluctant to perform any securities assessment or studies. Because they found it difficult to assess the vulnerability of their operational control system and to test and verify the performance of proposed security upgrades prior to installation. Besides, in order to protect reputation they would prefer to conceal it even if any security incident occurred. Therefore, it becomes more difficult to keep incident report and examine vulnerabilities analyzing in SCADA system used in critical infrastructures. Despite of the reluctance and difficulties, a small number of valuable studies have been done recently. In the section 3, the Industrial Security Incident Database which is only study in the field, and two comprehensive studies on control system information security are surveyed and some important results are discussed.

Today firewall and Intrusion Detection System (IDS) have became usual and almost mandatory for corporate networks. Correspondingly, firewall and IDS implementation is still under development. In the section 4, a firewall implementation for Modbus, which is control system communication protocol, are given as example.

2.0 LEGISLATION STUDIES ABOUT CRITICAL INFRASTRUCTURE IN THE UNITED STATES OF AMERICA AND THE EUROPEAN UNION

In USA, based on the recommendation of the Critical Infrastructure Working Group (CIWG), former USA president Bill Clinton set up the Presidential Commission on Critical Infrastructure Protection (PCCIP) in 1996, the first national effort to address the vulnerabilities. Presidential Decision Directives (PDD) 62 and 63 were issued after recommendation of the PCCIP. Those directives founded policy-making and oversight bodies making use of existing government agencies. PDD-63 aimed to develop plans to protect government-operated infrastructure and called for a dialog between the government and the private sector to develop a National Infrastructure Assurance Plan [4]. PDD 63 is also important because of being the first significant official policy which aims to take necessary measures to eliminate any significant vulnerability to both physical and cyber attacks on critical infrastructures in USA [5].

At the beginning of 2000s, most important event effect on changing security approach on critical infrastructure system in USA is September 11 attack. In response to this attack, *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT ACT 2001) is legislated by USA congress. According to the act, critical infrastructure defined as follow: “ Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters” [6].

Based on this definition, Homeland Security Presidential Directive 7 (HSPD-7), issued on December 2003, identified top 7 critical infrastructures and key resource and described the role and responsibilities for the protection of these sectors. The National Infrastructure Protection Plan, issued in 2006, and strategy for Homeland Security, issued in 2007, both reconfirm the HSPD-7 list of top 7 critical sectors [4]. One of the common features for all, which includes or relate, is control system like SCADA.

Two recent studies organized by USA Department of Energy and Department of Homeland Security after HSPD-7 issued surveyed in the section 3. These studies show that how much USA care about it as well as demonstrating SCADA security vulnerabilities.

In EU, The Communication of the Commission of the European Communities on Critical Infrastructure (CI) Protection in Fight Against Terrorism adopted on October 2004. In the Communication, CI are defined as follow: “ Critical infrastructure consist of those physical and information technology facilities, network, services and assets which, if disrupted or destroyed, would have a serious impact on health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States ” [7].

In November 2005, the Commission adopted a Green Paper on a European Programme for Critical Infrastructure Protection (EPCIP) which provided policy options on how the Commission could establish EPCIP and CIWIN (Critical Infrastructure Warning Information Network) [8].

As part of the EPCIP framework dealing specifically with European Critical Infrastructures, it is necessary to include a proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection. The proposed Directive establishes the necessary procedure for the identification and designation of European Critical Infrastructure (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructure [9].

EU Commission also suggest following factors to determine the criticality of an infrastructure. These factors are given below [9]:

- *Scope* - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.
- *Severity* - The degree of the loss can be assessed as None, Minimal, Moderate or Major.
- *Effects of time* - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

EPCIP does not put forward any concrete protection measures. The ECI Directive establishes a procedure leading to the identification of protection gaps.

Many country and international organization became aware of importance of critical infrastructure security. In order to provide different infrastructure security need, they have taken various measures and, make laws and regulations. In this section, since it is impossible to say about all county and organization, USA and EU were selected as examples to review legislative studies. In the most of critical infrastructures like energy, water production distribution or chemical, nuclear industrial plant, SCADA system is used to control all processes. To make sure security of critical infrastructures, it should be ensure SCADA system security.

3.0 RECENT AND COMPREHENSIVE STUDIES AND REPORTS ON SCADA/DCS SECURITY

3.1 SCADA Security Incident Database Study

In 2001, two researcher at British Columbia Institute of Technology (BCIT), Eric Byres and David Leversage, founded the Industrial Security Incident Database (ISID) aiming to serve as industry-wide repository for collecting, analyzing and sharing high-value information regarding cyber security incidents that directly affect SCADA, manufacturing and process control systems [10]. ISID, saving 116 SCADA security incident occurred between 1982 and 2006, is leading database in literature.

Figure 1 given below shows percentage of reported incident happened between 2002 and 2006.

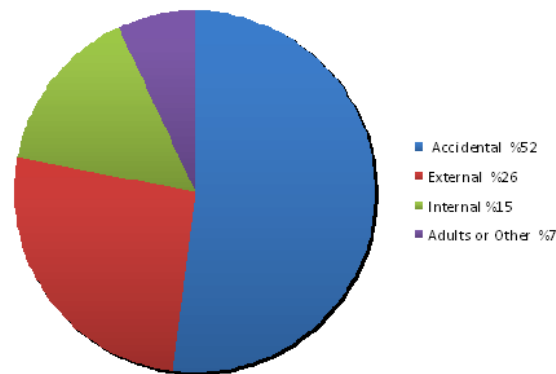


Figure.1 Incident types charted as a percentage from 2002 to 1 June 2006

On the other hand, figure 2 shows percentage of reported incident happened between 1982 and 2001.

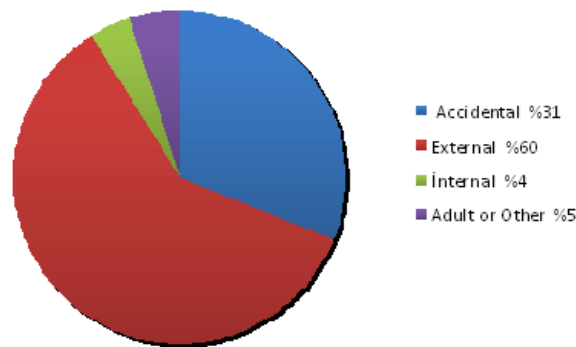


Figure.2 Incident types charted as a percentage from 1982 to 2001 [10]

According to ISID, percentage of reported incident happened between 2002 and 2006 is %73 while only %27 incident happened between 1982 and 2001 [10]. These results clearly point that there is a significant increase in the annual incident rate starting in late 2001. Another study on ISID indicates that %60 of all event during the period 2002 to 2006 were externally generated [10].

Significant change in threat source is easily seen when Figure 1 and Figure 2 are compared.

SCADA Security incidents published by prominent newspaper and magazine in USA and Europe verifies ISID studies. Several published well-known security incidents are given below.

- In January 1998, hackers seized control of GazProm's gas pipeline system [11].
- In 2000, Vitek Boden, former contractor manipulated the SCADA system of Hunter Watertech in Maroochy Shire, Australia. He released one million liters of untreated sewage to the environment [12].
- In November 2001, a SCADA software error in the Netherland caused natural gas to be produced with the incorrect composition; 26000 Dutch households were unable to heat their homes for three days [11].
- In January 2003, the SQL worm shut down communications at an electric power substation in the United States. The same worm affected the telemetric system of SCADA facility and attacked a security display station at the Davis-Besse nuclear power plant [11].
- According to news of The Washington Post, on 7 March 2008 at Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, a software update on a computer on the plant's business

network cause safety systems to errantly interpret the lack of data as a drop in water reservoirs that cool the plant's radioactive nuclear fuel rods. As a result, automated safety systems at the plant triggered a shutdown [13].

- According to news published by The Wall Street Journal on 5 April 2009, Cyberspies have penetrated the USA electrical grid and left behind software programs that could be used to disrupt the system [14].

Apart form ISID, there is still no well-documented incident database worldwide. This makes it difficult to assess potential attacks. But ISID database indicates only rate and change of attack types.

In the following section 3.2, two valuable reports are studied to better understand recent vulnerabilities.

3.2 Survey on Recent Two Studies on Control System Information Security

NSTB (National SCADA Test Bed), founded by USA Department of Energy Office of electricity Delivery and Energy Reliability, is a program to help the energy sector and equipment vendors assess control systems vulnerability and test the security of control systems hardware and software [15]. NSTB is a multi-laboratory partnership that draws on integrated expertise and resource of Argonne, Idaho, Oak Ridge, Pasific Northwest, and Sandia National Laboratories [16].

The Common Cyber Security Vulnerability Observed in Control System Assessment by INL NSTB report, prepared by Idaho National Laboratory (INL) in 2008, depict that cyber security assessments of control systems conducted on behalf of NSTB program. This report present 16 control system assessments performed from 2003 through 2007 [15]. Information found in this report could benefit vendors, asset owners, academicians, and other stakeholders. INL-NSTB 2008 report is also important in terms of representing methods for mitigating currents vulnerabilities as well as new technologies and approaches being developed in response to security challenges.

The assessment findings described in INL- NSTB 2008 report are organized to security dimension and category in which they belong. Basic security dimensions respectively defined in the report are Security Group (SG) Knowledge, Attack Group (AG) Knowledge, Access, Vulnerability [15].

In INL- NSTB 2008 report, security group knowledge dimension were divided into two categories with common vulnerabilities. First one is that management deficiencies led to legacy network access rules not being removed from firewall and routers, which allowed access paths to hosts and ports that were no longer needed. Second is documentation deficiencies resulted in inaccurate critical asset documentation. Table 1 shows frequency of SG knowledge common vulnerability found during assessments.

Table 1. Frequency of security group knowledge common vulnerabilities by category [15].

Vulnerability Category	Number of Unique Detailed Finding Descriptions
Documentation Deficiency	4
Change Management Deficiency	3

Deficiencies defined in same reports led to unauthorized access to information about target system by attack group are unencrypted services. In addition, there categories with common vulnerabilities were identified in

the access security dimension: firewall filtering deficiencies, remote access, and physical access. Figure 3 shows frequency of access dimension common vulnerabilities according to these three categories.

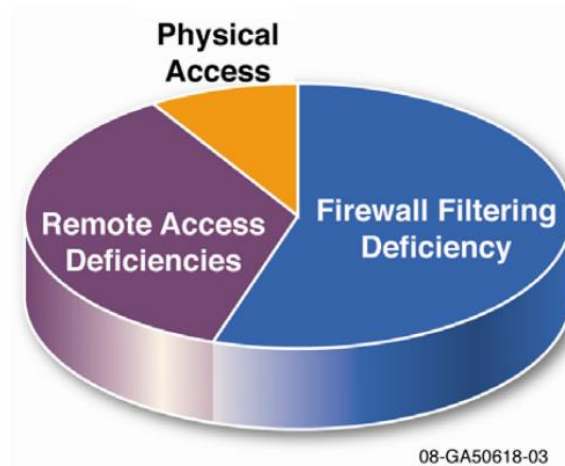


Figure. 3 Frequency of access dimension common vulnerabilities by category [15].

According to INL- NSTB 2008 report, the vulnerability security dimension is that dealing with weaknesses in control systems that allows an attacker to advance towards or accomplish malicious objectives. Defined vulnerabilities in the vulnerability security dimension are lack of input validation, weak user authentication, least privileges not enforced, unpatched systems. Figure 4 depicts frequency of vulnerability dimension common vulnerabilities by category.

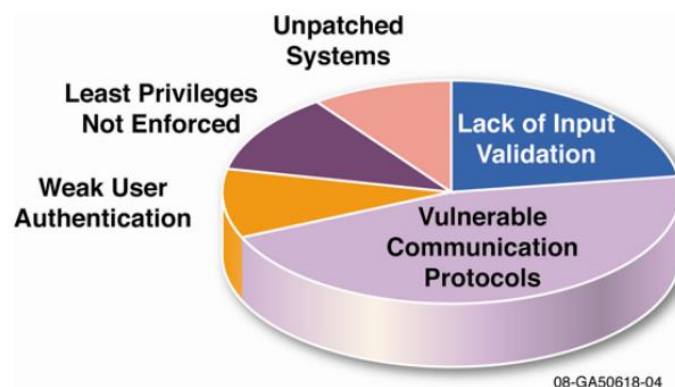


Figure. 4 Frequency of vulnerability dimension common vulnerabilities by category [15].

Similar to INL- NSTB 2008 report, Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessment is another comprehensive and recent report on SCADA / DCS security, prepared by USA Department of Homeland Security (DHS) National Cyber Security Division's Control System Security Program (CSSP). CCSP 2009 report presents results from 15 control systems assessments from 2004 through 2008. Once this report identifies vulnerabilities that could put critical infrastructure at risk for a cyber attack, mitigation strategies are developed to enhance control systems (CS) security [17].

In the CCSP 2009 report, common control systems vulnerabilities found CSSP security assessment are grouped into nine general security problem. Table 2 lists common CSSP assessments finding.

Table 2 Summary of common CSSP Control System assessment findings [17].

Category	Common Vulnerability
Poor code Quality	Use of potentially dangerous function in proprietary CS application
Vulnerable Web Services	Poor authentication
	Directory traversal enabled
	Unauthenticated access to Web server
Poor Network Protocol Implementations	Lack of input validation: Buffer overflow in CS service
	Lack of input validation: Lack of bounds checking in CS service
	CS protocol uses weak authentication
	CS product relies on standard Information Technology protocol that uses weak encryption
Poor Patch Management	Unpatched or old version of third-party application incorporated into CS software
	Unpatched operating systems
Weak Authentication	CS uses standard IT protocol that uses weak encryption
	Use of standard IT protocol with clear-text authentication
	Client-site enforcement of server-side security
	Improper security configuration
	No password required
	Weak password
	Weak password requirements
Least User Privileges Violation	Unauthorized directory traversal allowed
	Services running with unnecessary privileges
	Unencrypted proprietary CS protocol communication

Information Disclosure	Unencrypted nonproperty CS protocol communication
	Unencrypted services common in IT systems
	Open network shares on CS hosts
	Weak protection of user credentials
	Information leak through insecure service configuration
Network Design Vulnerabilities	Lack of network segmentation
	Firewall bypassed
Network Component Configuration Vulnerabilities	Access to specific ports on hosts not restricted to required IP address
	Port security not implemented on network equipment

Figure 5 shows the percentage of CSSP assessment finding for each category in Table 2

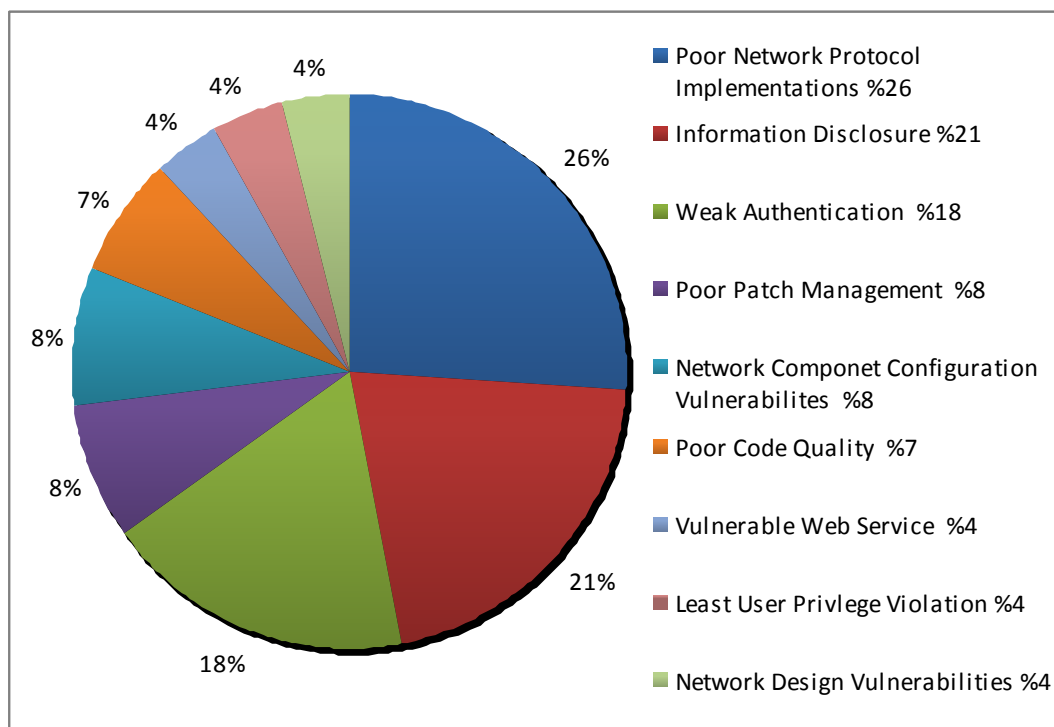


Figure. 5 Percentage of CSSP assessment finding in each vulnerability category [17]

CSSP 2009 report presents significant results for each different assessment category. The report denotes that totally 245 security vulnerabilities were found during all assessment. But, according to non-disclosure

agreements there is no information about what vulnerability in which infrastructure or vendors in the report.

Both CSSP 2009 and INL-NSTB 2008 are very significant, comprehensive and up-to-date report. All of them point out serious security risk on control systems in detail.

Although all reports aforementioned in this chapter/section offer some mitigation procedures and mention how to design more secure product and network, there are no practical solution to make legacy systems more secure.

Some communication protocols like Modbus, Profibus, DNP3 are still used widely in control system network. These protocols will continue to be used in the future by reason of economy and backward compatibility; however, new and more secure protocols are designed. Therefore Modbus, Profibus, DNP3 aware firewall and Intrusion Detection / Prevention System should continue to be developed.

4.0 A FIREWALL IMPLEMENTATION FOR MODBUS CONTROL SYSTEM COMMUNICATION PROTOCOL

Modbus is a simple request-response communication protocol commonly used in SCADA system. Modbus requests and responses flowing between client and server are encoded Modbus Protocol Data Units (PDU), which may be encapsulated in a serial line communication protocol, or in TCP/IP [18].

Although Modbus is originally developed for serial connections, TCP/IP functionality has been added to it as TCP/IP has become ubiquitous. So, all of the advantages and disadvantages of TCP/IP are now present in Modbus/TCP.

Bayindir et al.[19] developed energy monitoring system in the Department of Electrical Education of Gazi University in Turkey having 50 kW power in total and in use since November 2007. The energy monitoring system mainly consists of an energy analyzer and a PLC having VxWorks operating system. Since the Modbus protocol is supported by both devices, it was selected as communication protocol [19].

In another study followed a previous one, Bayindir et al.[20] put a Modbus aware firewall based on Linux Netfilter into energy monitoring system in order to prevent unauthorized access and certain Modbus function code. To implement this firewall, *libipt_modbus.c* file of ModbusFw open source project is put in iptables / netfilter firewall [20]. Figure 6 illustrates Modbus aware firewall, which is connected to both monitoring computer and power track system.

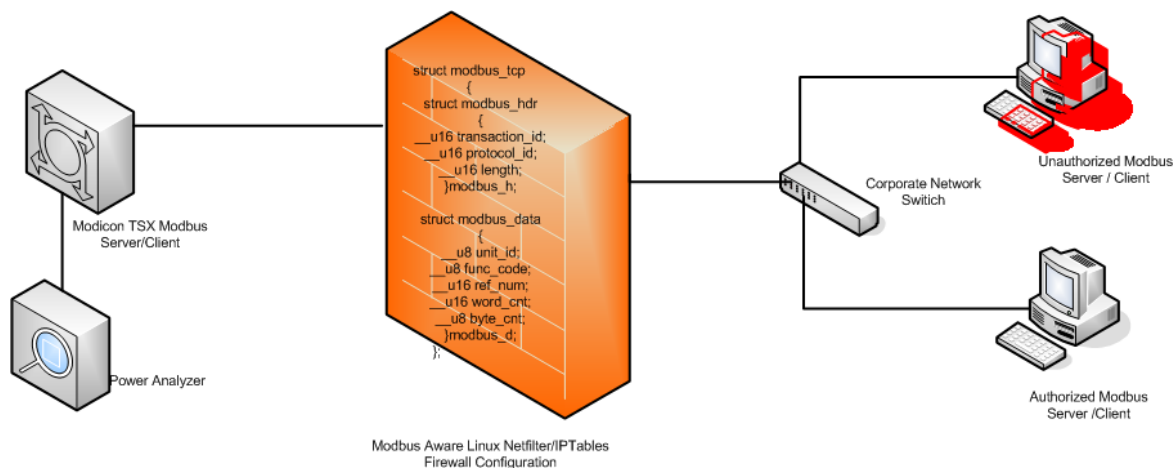


Figure. 5 Modbus aware firewall between monitoring computer and power track system

Similar to corporate network and internet based protocol like web, SMTP (Simple Mail Transfer Protocol), FTP (File Transfer Protocol), function of control system protocol like Modbus could easily filtered according to security policy of system. But installation and configuration of Modbus aware firewall is not easy as much as the other firewall. In addition, firewall or intrusion detection systems for the other most used control system communication protocol and their all functionalities have not developed yet.

5.0 DISCUSSION AND CONCLUSION

SCADA systems or distributed control systems are widely utilized in industries plant or infrastructure like electric/water/gas production or distribution systems, traffic signaling or mass transit systems, environmental control systems that have critical functions of countries around the world. In the other words, in case of disruption or destruction of these critical services, catastrophic events might be occurred.

Despite of some effort, there is no enough study on vulnerabilities detection. In some country like USA, governmental agencies support SCADA security assessment program. But, most of country have not prepared yet special program in order to assess security needs and criticality of infrastructures.

Various studies and assessments like CSSP 2009 and INL-NSTB 2008 mentioned in this study have revealed that there is a lack of security in SCADA systems. In order to moderate vulnerabilities, all participant including standardization organization, regulator bodies, vendors and network operators should work together to develop incident databases. Because incident databases in control system is one of the guidance for assessing main security vulnerabilities. Unfortunately there is no up to date, worldwide and open incident database.

Although SCADA systems have historically been isolated from other computer system like enterprise computer network, it have been interconnecting with enterprise network or internet by spreading with TCP/IP as a carrier protocol. In addition, general purpose operating system like Windows and Linux have started to be used mostly in new SCADA system. This have been led to emerge new vulnerabilities while property OS have been incapable of performing emerging security mechanism.

Control system communication protocol like Modbus, Profibus, DNP are still used widely in control system network, even though some more secure protocol or version are developed. Existing vulnerable

protocols will continue to be used in the future by reason of economy and backward compatibility; however, new and more secure protocols are designed. Therefore Modbus, Profibus, DNP3 aware firewall and Intrusion Detection / Prevention System should continue to be developed. Another security mechanism, which can be applied externally on existing infrastructure, should be developed as well.

Another problem, beyond technical capabilities of infrastructure element, is lack of strict security policy including weak protection of user credentials, Information leak through insecure service configuration, services running with unnecessary privileges as well as unauthorized physical access to devices. It must also ensure that only authorized parties have access to system, services and sensitive information about system structure and elements.

Comprehensive strategy for cyber attacks against the nation's critical infrastructure requires understanding the nature of the threats. Such strategy could be just only done if governmental agencies support. Therefore, public and private partnership is necessary to create depth defense and proactive solutions in terms of improving the security of SCADA control systems.

6.0 REFERENCES

- [1] Lewis T.G. (2006). *Critical Infrastructure Protection In Homeland Security*. Willey-Interscience, chapter-1.
- [2] The Department of Energy Office of Electricity Delivery and Energy Reliability (2009). *Fact Sheet: National SCADA Test Bed*.
http://www.oe.energy.gov/DocumentsandMedia/NSTB_Fact_Sheet_FINAL_09-16-09.pdf
- [3] Chandia R., Gonzalez J., Kilpatrick T., Papa M. & Sheno S. (2007). *Security Strategies for SCADA Networks*. Critical Infrastructure Protection, Springer Boston, Pages: 117-131.
- [4] Brunner E. & Manuel Suter M. (2008). *International CIIP Handbook 2008/2009: An Inventory of 25 National and 7 International Critical Information Infrastructure Protection Policies*, Center for Security Studies, ETH Zurich, Volume:4, Issue:1.
http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663
- [5] USA Presidential Decision Directive 63. (1998). *The Clinton Administration's Policy on Critical Infrastructure Protection*.
http://www.justice.gov/criminal/cybercrime/white_pr.htm
- [6] Moteff J. & Parfomak P. (2004). *Critical Infrastructure and Key Assets: Definition and Identification*. Congressional Research Service Reports, Order Code RL32631.
<http://www.fas.org/sgp/crs/RL32631.pdf>
- [7] Europa Justice and Home Affair. (2006). *EPCIP European Programme for Critical Infrastructure Protection*.
http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm
- [8] Commission Of The European Communities. (2006). *Communication From The Commission On A European Programme For Critical Infrastructure Protection*. Communication From The Commission, COM(2006) 786 Final, Brussels.
http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf
- [9] Commission Of The European Communities. (2005). *Green Paper On A European Programme For Critical Infrastructure Protection*. Communication From The Commission, COM(2005) 576

- final, Brussels.
http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf
- [10] Byres E. & Leversage D.(2006). *Security Incidents and Trends In Scada And Process Industries*. British Columbia Institute of Technology.
<http://www.processonline.com.au/articles/30300-Trends-in-security-incidents-in-the-SCADA-and-process-industries-a-summary-Part-1>
- [11] Christiansson H. & Luijff E. (2007). *Creating a European SCADA Security Testbed*. Critical Infrastructure Protection, Springer Boston Volume 253/2007,Pages: 237-247.
- [12] Slay J. & Miller M. (2007). *Lessons Learned From the Maroochy Water Breach*. Critical Infrastructure Protection Volume 253/2007, Springer Boston, November, Pages 73–82.
- [13] Krebs B. (2008). *Cyber Incident Blamed for Nuclear Power Plant Shutdown*. The Washington Post, June 5, 2008.
<http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html>
- [14] Gorman S. (2009). *Electricity Grid in U.S. Penetrated By Spies*. The Wall Street Journal, April 8, 2009.
<http://online.wsj.com/article/SB123914805204099085.html>
- [15] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. (2008). *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program*.
http://www.controlsystemsroadmap.net/pdfs/INL_Common_Vulnerabilities.pdf
- [16] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability. (2009). *SCADA National Test Bed Fiscal Year 2009 Work Plan*.
http://www.oe.energy.gov/DocumentsandMedia/FY09_Work_Plan_External.pdf
- [17] The U.S. Department of Homeland Security National Cyber Security Division's Control Systems Security Program (CSSP). (2009). *Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments*.
http://www.us-cert.gov/control_systems/pdf/DHS_Common_Vulnerabilities_R1_08-14750_Final_7-1-09.pdf
- [18] S. Cheung B., Dutertre M, Fong U., Lindqvist K.S. & A. Valdes. (2007) . *Using Model-based Intrusion Detection for SCADA Networks*. SCADA Security Scientific Symposium, Miami, FL.
- [19] Bayındır R., Irmak E., Çolak İ. and Bektaş A.(2008). *Development of a Real Time Energy Monitoring Platform*. Electrical Power and Energy Systems, submitted paper.
- [20] Bayındır R., Sağiroğlu S., Colak I., Ozbilen A.(2009). *Investigating Industrial Risks Based On Information Security For Observerable Electrical Energy Distribution System And Suggestions*. Journal of The Faculty of Engineering and Architecture of Gazi University. Cilt 24, No 4, 715-723, 2009 Vol 24, No 4, 715-723.